CLAIMS

What is claimed is:

1. A method of preventing an attack on a network, the method comprising the computer-implemented steps of:

receiving an ICMP packet that includes a copy of a header associated with a connection in a connection-oriented transport protocol;

obtaining a packet sequence value from the header;

determining if the packet sequence value is valid;

updating a parameter value associated with the transport protocol connection only if the packet sequence value is determined to be valid.

2. A method as recited in Claim 1, wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that includes a copy of a TCP header associated with a TCP connection.

3. A method as recited in Claim 1, wherein the step of receiving an ICMP packet comprises receiving an ICMP "endpoint unreachable" error packet.

4. A method as recited in Claim 1, wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that specifies that fragmentation is needed.

5. A method as recited in Claim 1, wherein the step of determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of packet sequence values that are allowed by the transport protocol for the connection.

6. A method as recited in Claim 1, wherein the step of determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of sent but unacknowledged TCP packet sequence values for the connection.

7. A method as recited in Claim 1, wherein the step of determining if the packet sequence value is valid comprises determining if the packet sequence value is exactly equal to one or more sequence values of one or more packets that are then-currently stored in a TCP re-transmission buffer, starting at a sequence value of a previously sent segment that resulted in receiving the ICMP packet.

8. A method as recited in Claim 1, wherein the steps are performed in a router acting as a TCP endpoint node.

9. A method as recited in Claim 1, wherein the steps are performed in a firewall device.

10. A method of preventing an attack on a network, the method comprising the computer-implemented steps of:

receiving, at a TCP endpoint node in a TCP/IP packet-switched network, an ICMP packet that includes a copy of a TCP header associated with a TCP connection;

obtaining a packet sequence number from the TCP header;

determining if the packet sequence number is valid;

updating a maximum transmission unit (MTU) value associated with the TCP connection only if the packet sequence number is determined to be valid.

11. A method as recited in Claim 10, wherein the step of receiving an ICMP packet comprises receiving an ICMP "endpoint unreachable" error packet.

12. A method as recited in Claim 10, wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that specifies that fragmentation is needed.

13. A method as recited in Claim 10, wherein the step of determining if the packet sequence number is valid comprises determining if the packet sequence number is within a range of TCP packet sequence numbers that are allowed for the connection.

14. A method as recited in Claim 10, wherein the step of determining if the packet sequence value is valid comprises determining if the packet sequence number is within a range of sent but unacknowledged TCP packet sequence values for the connection.

15. A method as recited in Claim 10, wherein the step of determining if the packet sequence value is valid comprises determining if the packet sequence number is equal to one or more sequence numbers of one or more packets that are then-currently stored in a TCP re-transmission buffer, starting at a sequence value of a previously sent segment that resulted in receiving the ICMP packet.

16. A method as recited in Claim 10, wherein the steps are performed in a router acting as a TCP endpoint node.

17. A method as recited in Claim 10, wherein the steps are performed in a firewall device.

18. A computer-readable medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of any of claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, or 17.

19. Apparatus for preventing an attack on a network, comprising:

means for receiving an ICMP packet that includes a copy of a header associated with a connection in a connection-oriented transport protocol;

means for obtaining a packet sequence value from the header;

means for determining if the packet sequence value is valid;

means for updating a parameter value associated with the transport protocol connection only if the packet sequence value is determined to be valid.

20. An apparatus as recited in Claim 19, wherein the means for receiving an ICMP packet comprises means for receiving an ICMP packet that includes a copy of a TCP header associated with a TCP connection.

21. An apparatus as recited in Claim 19, wherein the means for receiving an ICMP packet comprises means for receiving an ICMP "endpoint unreachable" error packet.

22. An apparatus as recited in Claim 19, wherein the means for receiving an ICMP packet comprises means for receiving an ICMP packet that specifies that fragmentation is needed.

23. An apparatus as recited in Claim 19, wherein the means for determining if the packet sequence value is valid comprises means for determining if the packet sequence value is within a range of packet sequence values that are allowed by the transport protocol for the connection.

24. An apparatus as recited in Claim 19, wherein the means for determining if the packet sequence value is valid comprises means for determining if the packet sequence value is within a range of sent but unacknowledged TCP packet sequence values for the connection.

25. An apparatus as recited in Claim 19, wherein the means for determining if the packet sequence value is valid comprises means for determining if the packet sequence value is equal to one or more sequence values of one or more packets that are then-currently stored in a TCP re-transmission buffer.

26. An apparatus as recited in Claim 19, comprising a router acting as a TCP endpoint node.

27. An apparatus as recited in Claim 19, comprising a firewall device.

28. A network element, comprising:
a network interface that is coupled to a data network for receiving one or more packet flows therefrom;
a processor;
one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of any of claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, or 17.